

Program guidelines

Program highlights

 Platform Standards

Fully compliant with Platform Standards. [🔗](#)

 Top Response Efficiency

This program's response efficiency is above 90%. [🔗](#)

Managed by HackerOne



18 hours

Average time to first response



1 day,
13 hours

Average time to triage



2 weeks,
4 days

Average time to bounty



2 weeks,
5 days

Average time from submission to bounty

Rewards summary

Last updated on June 25, 2024. [View changes](#) [🔗](#)

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable.

Low	Medium	High	Critical
Avg. bounty \$66 29.65% submissions	Avg. bounty \$441 29.25% submissions	Avg. bounty \$1,256 28.88% submissions	Avg. bounty \$2,500 12.23% submissions
\$50	\$400	\$1,000–\$3,000	\$3,000–\$5,000

Where monetary bounty is presented, eligible reports will be awarded based on our Awarding Process. For further details please review them under our policy section.

[Learn more about HackerOne](#)[Log in](#)

Focus Assets in scope:

- att.com/msapi
- att.com/buy/
- att.com/acctmgmt/
- myattwg.att.com/olam/
- myATT mobile apps
- signin.att.com
- identity.att.com

Scope exclusions

Core Ineligible Findings are out of scope. [Learn more](#) [↗](#)

Overview

Last updated on June 16, 2025. [View changes](#) [↗](#)

AT&T Bug Bounty Program Policy

Welcome to the AT&T Bug Bounty Program! We now use a pay per vulnerability model and utilize the HackerOne platform!

UPDATE:

The following asset has been removed from scope as of 1/2/2025 SupplierGateway.
Removed from scope as of 11/16/2021 DIRECTVLA (Vrio Corp, SKY)

The Program encourages and rewards contributions by developers and security researchers who help make AT&T's public-facing online environment more secure. Through the Program AT&T provides monetary rewards and/or public recognition for security vulnerabilities responsibly disclosed to us.

The following explains the details of the Program. If you are new to our Program, please be sure to review the Program Guidelines, Program Exclusions, and Terms and Conditions, as well as the Reporting and Payment Process prior to making a submission.

Program Guidelines

SupplierGateway, Xandr, DIRECTVLA (Vrio Corp, SKY), WarnerMedia assets, including HBO, are out-of-scope of the AT&T program and are therefore ineligible for bounty rewards. A security vulnerability is generally an error, flaw, mistake, failure, or fault in a computer program or system that impacts the security of a device, system, network, or data. Any security vulnerability may be considered for the Program; however, it must be a new, previously unreported, vulnerability in order to be eligible for reward or recognition.

Typically, in-scope submissions will include high impact vulnerabilities. However, any vulnerability that could realistically place the online security of AT&T, our customers, or the public at large at risk is in scope and might be rewarded. Vulnerabilities which directly or indirectly affect the confidentiality or integrity of user data or privacy are prime candidates for a reward. Some characteristics that are considered when "qualifying" vulnerabilities include those that:

- Directly or indirectly affect the confidentiality or integrity of user data or privacy;
- Compromise the integrity of the system;
- Enable unauthorized access to significant data or resources;
- Enable the running of unauthorized code;
- Increase privileges or access beyond that which is intended;
- Interfere with or bypass security controls or mechanisms;
- Are exploitable (i.e. not purely theoretical);
- Can be launched remotely; and
- Could cause damage to a user's system.

Focus Assets in scope.

- att.com/msapi
- att.com/buy/
- att.com/acctmgmt/
- myattwg.att.com/olam/
- myATT mobile apps
- signin.att.com
- identity.att.com

Informative Reports

Submissions against the following assets are accepted but are not eligible for an award and will be closed as Informative.

- Preferred Dealer

Program Exclusions

The following categories of vulnerabilities are excluded from reward in the Program unless otherwise directed by AT&T:

- Attacks against AT&T infrastructure;
- Social engineering and physical attacks;
- Distributed Denial of Service attacks that require large volumes of data;
- 0-day vulnerabilities less than 30/60/90 days from patch release are ineligible for bounty;
- Provisioning and/or usability issues;
- Violations of licenses or other restrictions applicable to any vendor's product;
- Security vulnerabilities in third-party products or websites that are not under AT&T's direct control;
- Duplicate reports of security issues, including security issues that have already been identified internally;
- Tenant/cloud systems executing in an Internet Data Center (IDC), where AT&T is simply acting as the site host;
- Employee Resource Group (ERG) websites;
- Clickjacking reports against unauthenticated pages and/or static content resources;
- Reports of missing SPF records for domains with no MX record;
- Vulnerabilities that are a result of malware;
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited, or
- Issues determined to be low impact.
- Self-XSS involving a payload in headers or in the body of the request
- POST based Reflected XSS
- Vulnerabilities which require a social engineering component are excluded. i.e. presenting injected data to a user and expecting the user to click on an external link to complete the compromise
- Login/logout CSRF
- Content spoofing which depends on a social engineering element to succeed (such as an error page suggesting that a user take an action) is excluded
- Abandoned CNAME records require a social engineering component to successfully exploit, they are excluded unless there is an existing link from a company resource to the invalid CNAME

 Learn more about HackerOne[Log in](#)

DIRECTV assets should be reported directly to the DIRECTV security team at directv-bbp@mydirectv.com.

Please note:

- Do not submit reports related to DIRECTV assets to this AT&T program
- DIRECTV maintains a separate security process for handling vulnerability reports
- All DIRECTV-related security concerns should be directed exclusively to directv-bbp@mydirectv.com

In addition, the submitter:

- Must not be the author of the code with the vulnerability or
- Must not be employed by AT&T directly or indirectly.

Vulnerabilities that are disclosed to any party other than AT&T, including vulnerability brokers, will not qualify for reward. This includes both public disclosure and limited private release.

Program Terms and Conditions

The following Terms and Conditions apply to the Program:

- "AT&T" refers to AT&T Services, Inc., and its affiliates.
- You must comply with the Program and abide by the law.
- AT&T employees, contractors, and their families are not eligible for rewards.
- You must submit your report as soon as you have discovered a potential vulnerability. By submitting the vulnerability, you affirm that you have not disclosed and agree that you will not disclose the vulnerability or your submission to anyone other than AT&T following the process set forth in the Program. Absent AT&T's prior written consent, any disclosure would violate the Program. It is understood and agreed that money damages would not be a sufficient remedy for any breach of this paragraph by you or your representative(s) and that AT&T shall be entitled to specific performance as a remedy for any such breach, including injunctive relief. Such remedy shall not be deemed to be the exclusive remedy for any such breach but shall be in addition to all other remedies available at law or equity to AT&T.
- Submissions selected for rewards, and the individuals who submitted the vulnerabilities will receive recognition at the sole discretion of AT&T.
- By submitting information about a potential vulnerability, you agree to all Program Terms and Conditions and grant AT&T a worldwide, royalty-free, non-exclusive

 Learn more about HackerOne[Log in](#)

- Eligibility for rewards, including the determination of the recipients and reward amount is left up to the sole discretion of AT&T.
- Out of scope vulnerabilities submitted are generally less likely to receive recognition or rewards under the Program.
- You are responsible for all taxes associated with and imposed on any reward you may receive in connection with your submission. HackerOne handles all bounty payments through the HackerOne platform. Please refer to HackerOne's relevant policies [here](#).
- You may only exploit, investigate, or target vulnerabilities against your own accounts. Testing must not violate any law, or disrupt or compromise any data or access data that is not yours; intentional access of customer data other than your own is expressly prohibited.
- If you inadvertently access customer, employee, or business related information during your testing, you must immediately notify AT&T and the information must not be used, disclosed, stored, or recorded in any way. Inadvertent access of the data must be declared within your submission.
- Your testing activities must not negatively impact AT&T, or AT&T's Environment availability or performance.
- AT&T reserves the right of non-remediation in its sole discretion.
- The Program constitutes the entire agreement and understanding of the parties with respect to the items listed herein. The Program may be amended or modified any time without notice in AT&T's sole and absolute discretion.
- If any portion of the Program is found to be illegal or unenforceable, then the parties shall be relieved of their responsibilities arising under such portion, but only to the extent that such portion is illegal or unenforceable.

Reporting Process

When reporting vulnerabilities, you must first register or log on to your account on HackerOne. In describing the vulnerability it is important to include all necessary details required for reproducing the vulnerability as well as the tools required to reproduce the vulnerability. Please note that the vulnerability should be treated in accordance with the terms of the Program.

- Each submission will typically receive a reply within one (1) business day acknowledging that the report was successfully received.
- Duplicate submissions (where the vulnerability has already been reported to AT&T) are not eligible for rewards. In most instances, you will not be notified of a duplicate report condition until after the vulnerability has been remediated.

[Learn more about HackerOne](#)[Log in](#)

once the Program is notified by AT&T internal support team. AT&T cannot provide updates on remediation efforts that are in progress.

Awarding Process

Only vulnerabilities will be considered for an award. Only those vulnerabilities that have been resolved will receive an award. The bounties range from \$50 to \$3,000 depending on criteria such as the type/severity of the vulnerability, impacted domain(s), potential vulnerability exploits, and vulnerability report submission quality. In general, Reflected XSS will be considered low severity and awarded with minimum bounty unless other impact is shown. THE CRITERIA USED TO DETERMINE THE PAYOUT FOR A VULNERABILITY IS SOLELY AT THE DISCRETION OF AT&T.

Change to Program Terms

AT&T reserves the right to discontinue the Program at any time without notice in its sole discretion.

Top hackers

[See all hackers](#)

- | | | | |
|----|--|----|--|
| 1 |  r3aper__
Reputation: 17k | 2 |  f6x
Reputation: 10k |
| 3 |  diogourupes
Reputation: 9k | 4 |  ismailsenturk
Reputation: 8k |
| 5 |  trudya
Reputation: 5k | 6 |  todayisnew
Reputation: 4k |
| 7 |  nxnj
Reputation: 4k | 8 |  d0xing
Reputation: 4k |
| 9 |  caon
Reputation: 4k | 10 |  0xd0m7
Reputation: 3k |
| 11 |  melar_dev
Reputation: 3k | 12 |  chimoul
Reputation: 2k |

 Learn more about HackerOne

Log in



[Leaderboard](#)

[Status](#)

[Support](#)

[Press](#)

[Terms](#)

[Blog](#)

[Docs](#)

[Disclosure Guidelines](#)

[Privacy](#)



© HackerOne